THAT WHICH IS CLAIMED IS:

1. An electronic circuit for the securing of a coprocessor dedicated to cryptography comprising:
   - a memory module,
   - a battery of input/output registers
5 connected to the memory module by a two-way link,
   - a multiplexer to carry out a transfer of data between the battery of input/output registers and an input register or a key register, the input register and the key register respectively receiving the data
10 elements of a message to be processed by an encryption or decryption operation and the data elements of an encryption or decryption digital key,
   - a processing module to perform an encryption or decryption operation accepting, at a
15 first input, the messages to be processed contained in the input register and, at a second input, the digital key contained in the key register to process the message to be processed,
   - a control module to manage the operations
20 performed by the memory module, the battery of input/output registers, the multiplexer and the processing module,
   - an output register to transmit the result of an encryption or decryption operation to the battery
25 of input/output registers through the multiplexer, wherein the battery of input/output registers comprises a scrambling register to receive scrambling bits foreign to the message to be encrypted or decrypted and/or to the digital key.

2. An electronic circuit for the securing of a coprocessor dedicated to cryptography according to claim 1, wherein the circuit comprises an accessory

input register connected to the processing module and

5   to the multiplexer to receive the scrambling bits sent

directly by the processing module or coming from the

memory module.

3.   An electronic circuit for the securing of

a coprocessor dedicated to cryptography according to

claim 2, wherein the accessory input register is of the

same size as the scrambling register.

4.   An electronic circuit for the securing of

a coprocessor dedicated to cryptography according to

one of the preceding claims, wherein the scrambling

bits are generated randomly.

5.   An electronic circuit for the securing of

a coprocessor dedicated to cryptography according to

one of the preceding claims, wherein the scrambling

bits are sent in groups of eight bits.

6.   A method for the securing of a

coprocessor dedicated to cryptography comprising the

steps consisting in successively:

- transmitting data by means of a two-way

5   link from a memory module to a battery of input/output

registers

- transmitting, through a multiplexer, from

the battery of input/output registers respectively to

an input register and to a key register, respectively

10   data corresponding to a message to be processed by an

encryption or decryption operation and data

corresponding to an encryption or decryption digital

key,

- processing the message to be processed by

15   means of a processing module accepting, at a first

input, the data elements coming from the input register and, at a second input, the data elements coming from the key register and giving the data elements corresponding to the processed message to the output

20 register,

wherein the method according to the invention comprises the additional step consisting of the transmission, to a scrambling register of the battery of input/output registers, of the scrambling bits

25 foreign to the message to be processed and the transmission, to the digital key, of the scrambling bits being sent directly by the memory module or coming from the processing module.

7. A method for the securing of a coprocessor dedicated to cryptography according to claim 6, wherein the scrambling bits are transmitted

5 into an accessory register connected to the processing module and to the multiplexer to receive the scrambling bits sent directly by the processing module or coming from the memory module.

8. A method for the securing of a coprocessor dedicated to cryptography according to one of the claims 6 or 7, wherein the scrambling bits are transmitted randomly.

9. A method for the securing of a coprocessor dedicated to cryptography according to one of the claims 6 to 8, wherein scrambling bits are sent to the scrambling register whenever a digital key is

5 loaded into the battery of input/output registers.

10. A method for the securing of a coprocessor dedicated to cryptography according to one

of the claims 6 to 9, wherein the scrambling bits are
emitted in groups of eight bits.